FIG. 1

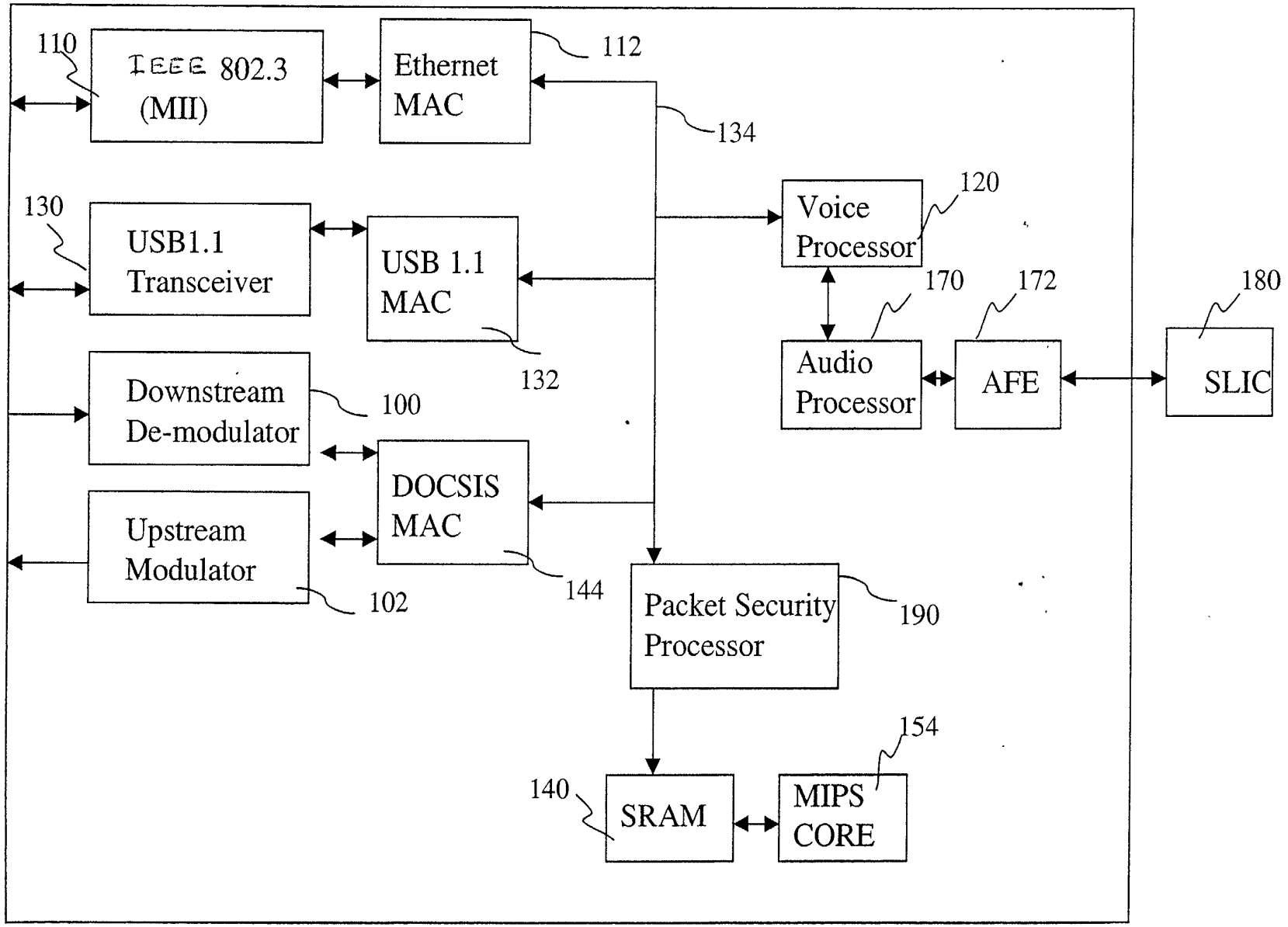

110
IEEE 802.3
(MII)
Ethernet
MAC
112
134
130
USB1.1
Transceiver
USB 1.1
MAC
132
120
Voice
Processor
170
172
180
Audio
Processor
AFE
SLIC
Downstream
De-modulator
100
DOCSIS
MAC
Upstream
Modulator
102
144
Packet Security
Processor
190
154
140
SRAM
MIPS
CORE

FIG. 2

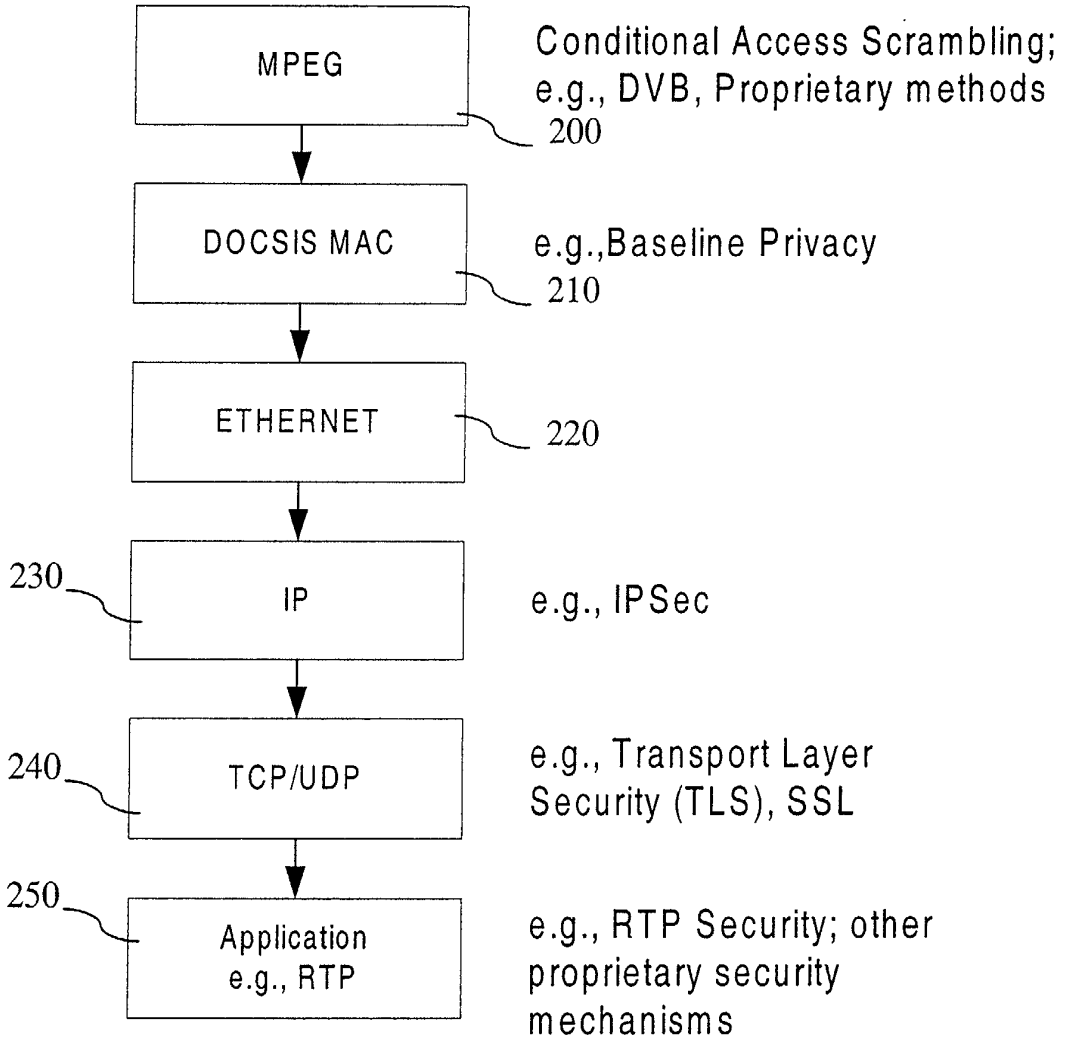
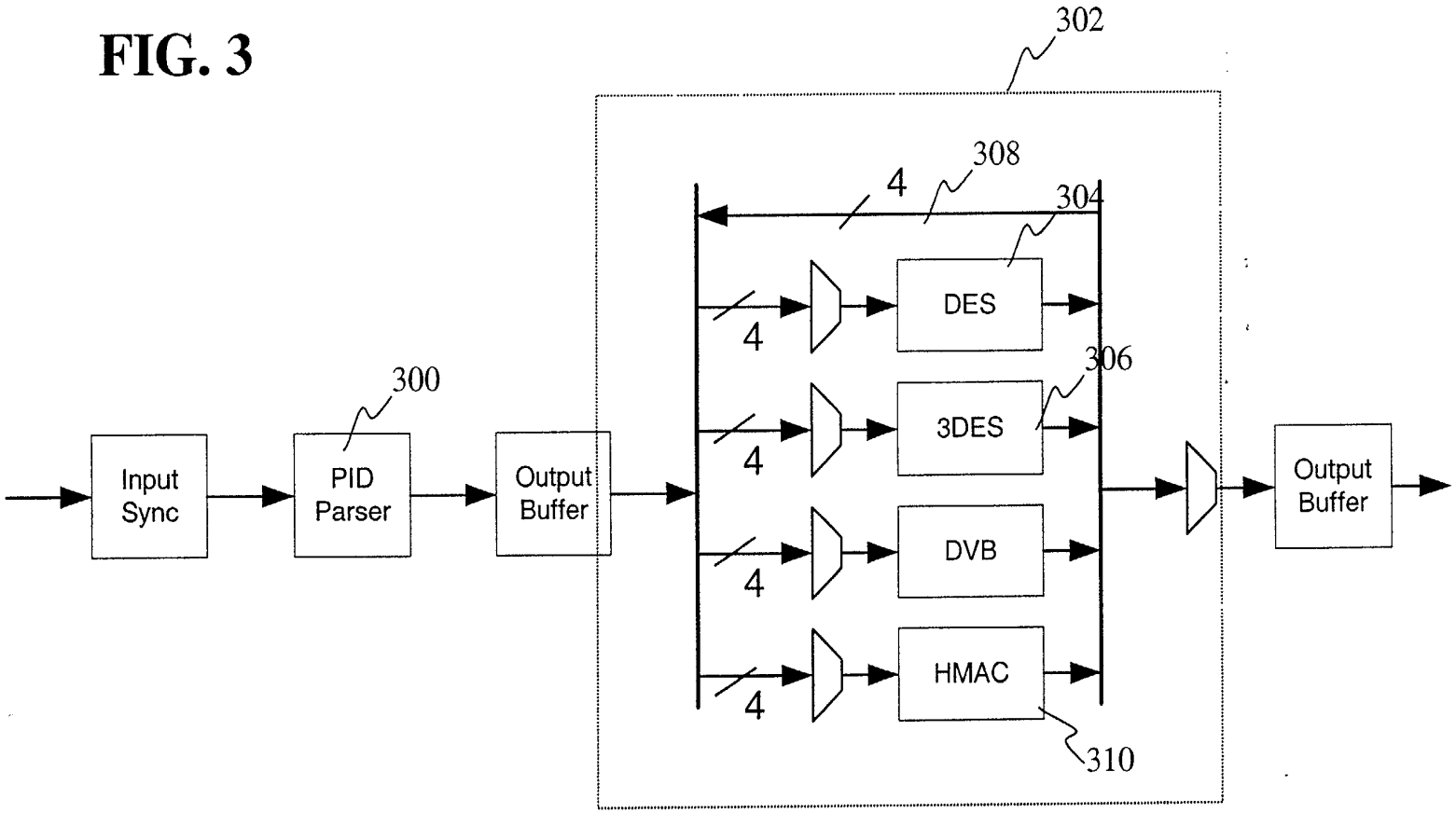
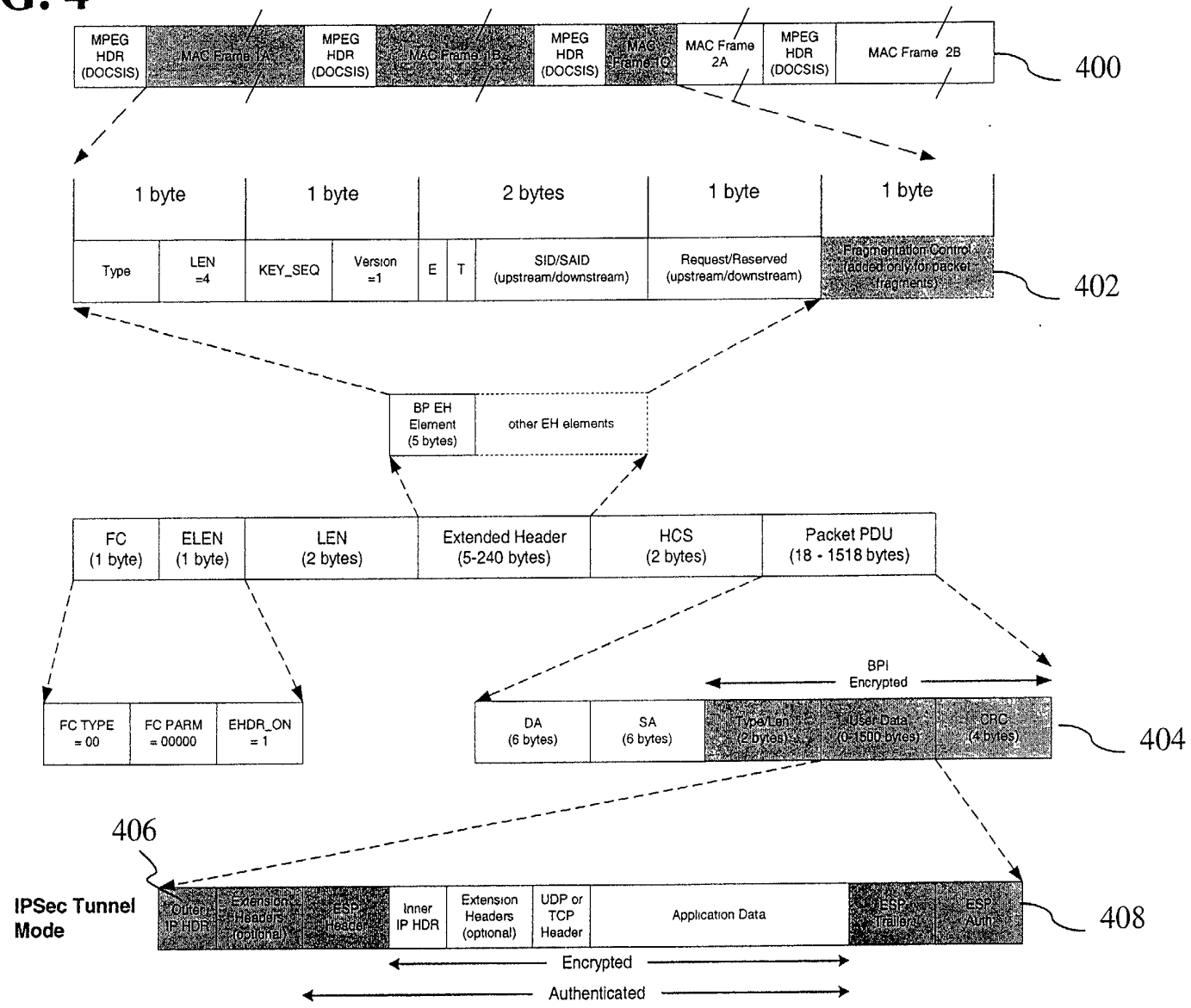

MPEG
Conditional Access Scrambling; e.g., DVB, Proprietary methods
200
DOCSIS MAC
e.g.,Baseline Privacy
210
ETHERNET
220
230
IP
e.g., IPSec
240
TCP/UDP
e.g., Transport Layer Security (TLS), SSL
250
Application e.g., RTP
e.g., RTP Security; other proprietary security mechanisms

FIG. 3


302
308
4
304
DES
4
306
3DES
4
DVB
4
HMAC
310
300
Input Sync
PID Parser
Output Buffer
Output Buffer

20020 "0C2902

FIG. 4



20020708050F

FIG. 5

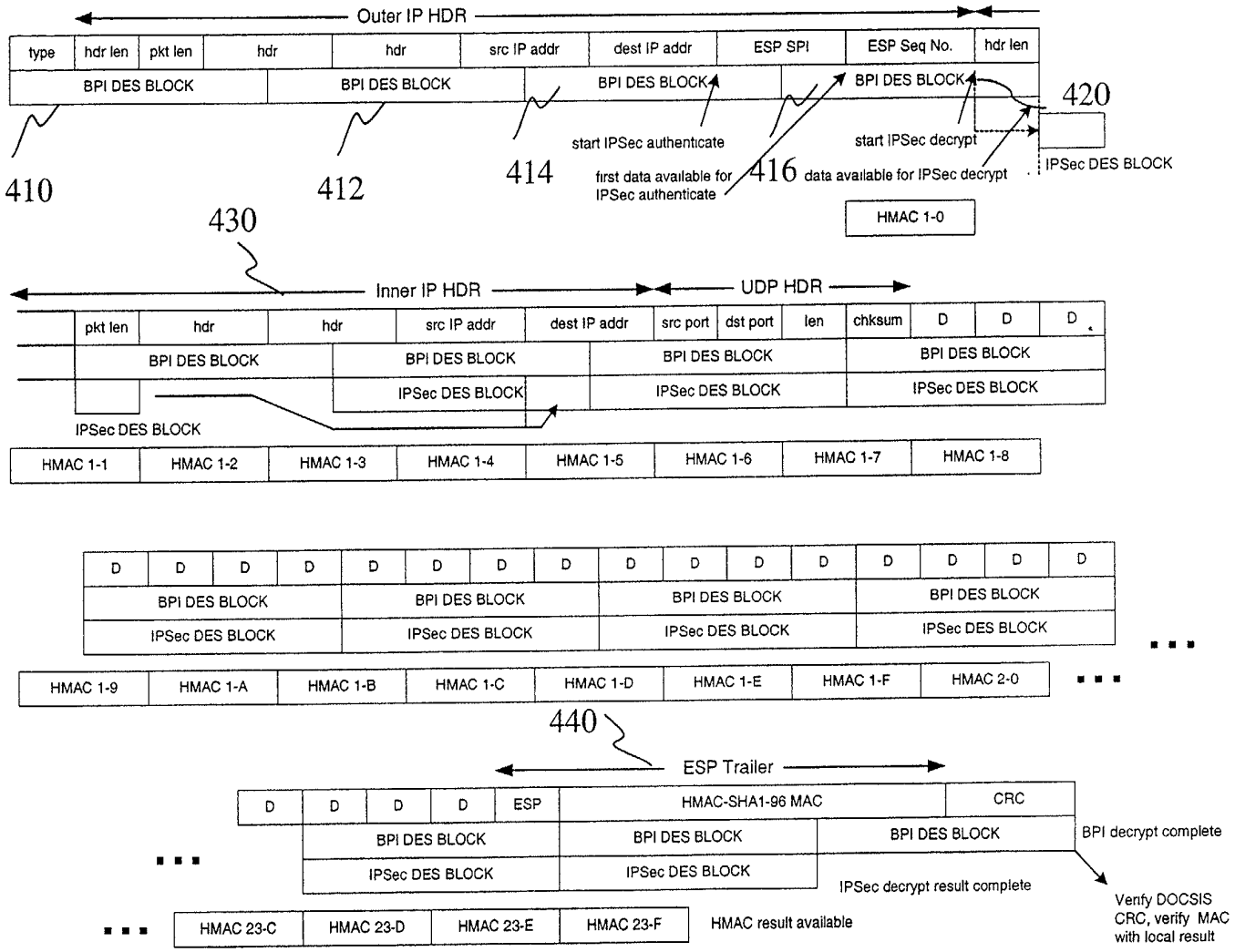
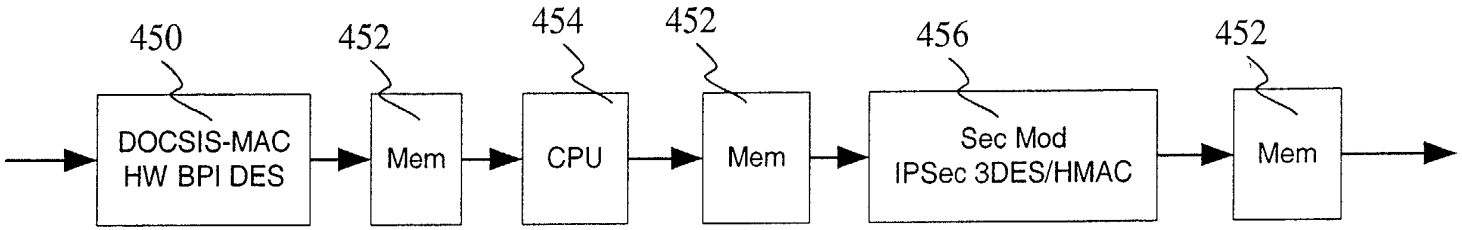
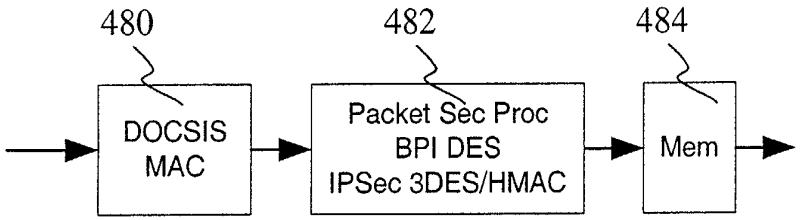


FIG. 6

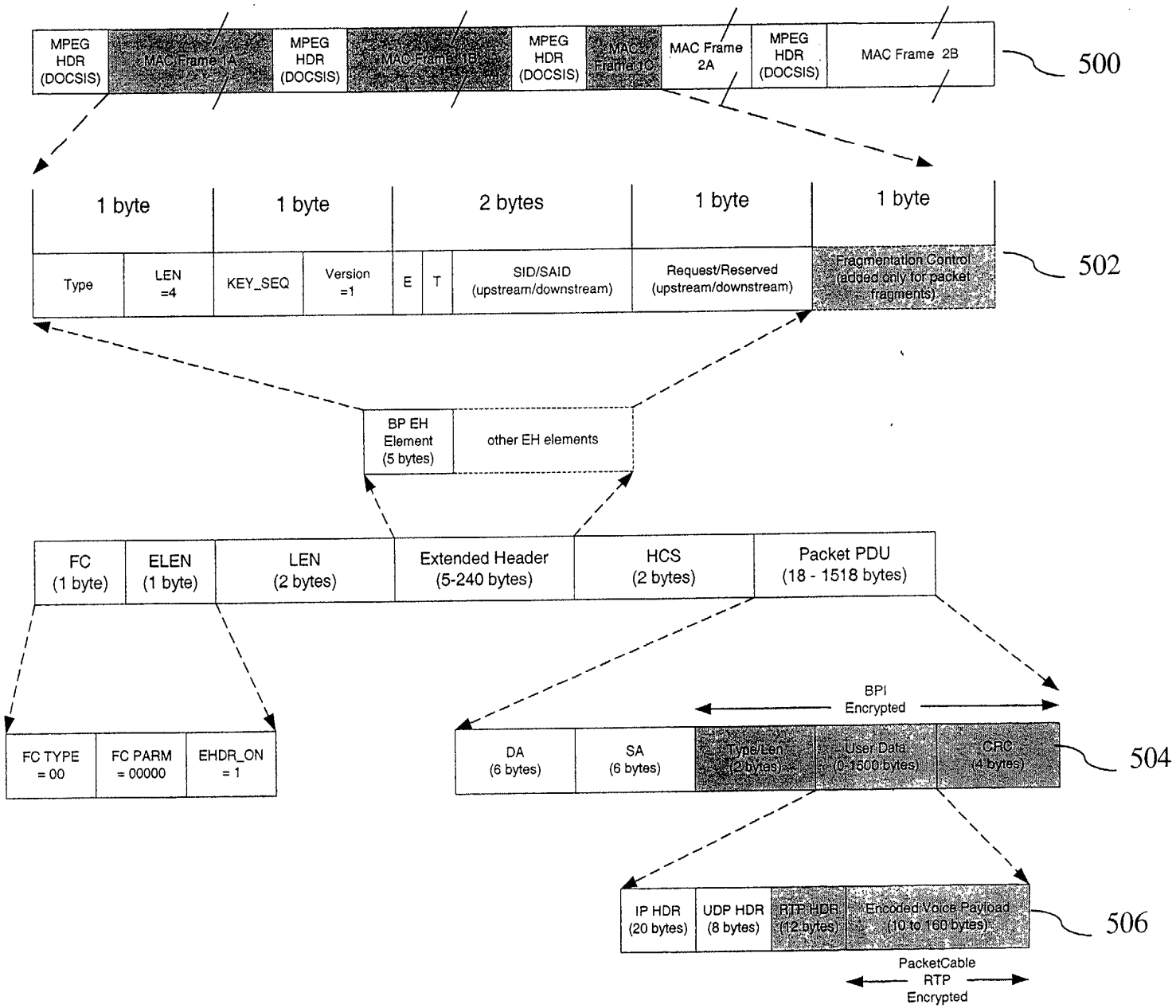


Current Process Flow



Converged Security Process Flow

FIG. 7


MPEG HDR (DOCSIS)
MAC Frame 1A
MPEG HDR (DOCSIS)
MAC Frame 1B
MPEG HDR (DOCSIS)
MAC Frame 1C
MAC Frame 2A
MPEG HDR (DOCSIS)
MAC Frame 2B
500
1 byte
1 byte
2 bytes
1 byte
1 byte
Type
LEN =4
KEY_SEQ
Version =1
E
T
SID/SAID (upstream/downstream)
Request/Reserved (upstream/downstream)
Fragmentation Control (added only for packet fragments)
502
BP EH Element (5 bytes)
other EH elements
FC (1 byte)
ELEN (1 byte)
LEN (2 bytes)
Extended Header (5-240 bytes)
HCS (2 bytes)
Packet PDU (18 - 1518 bytes)
FC TYPE = 00
FC PARM = 00000
EHDR_ON = 1
BPI Encrypted
DA (6 bytes)
SA (6 bytes)
Type/Len (2 bytes)
User Data (0-1500 bytes)
CRC (4 bytes)
504
IP HDR (20 bytes)
UDP HDR (8 bytes)
RTP HDR (12 bytes)
Encoded Voice Payload (10 to 160 bytes)
506
PacketCable RTP Encrypted

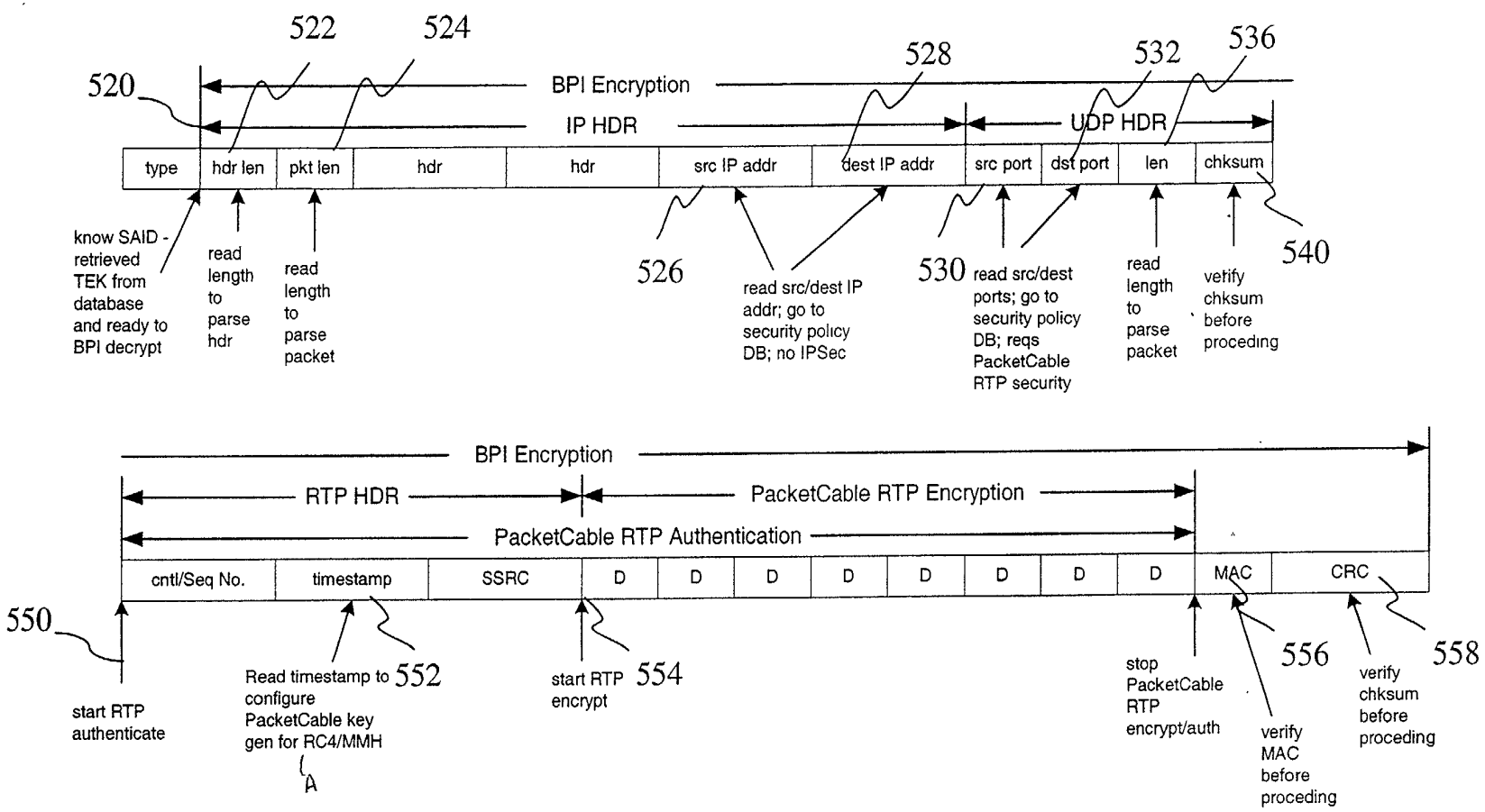

520
522
524
528
532
536
BPI Encryption
IP HDR
UDP HDR
type
hdr len
pkt len
hdr
hdr
src IP addr
dest IP addr
src port
dst port
len
chksum
540
know SAID - retrieved TEK from database and ready to BPI decrypt
read length to parse hdr
read length to parse packet
526
read src/dest IP addr; go to security policy DB; no IPSec
530
read src/dest ports; go to security policy DB; reqs PacketCable RTP security
read length to parse packet
verify chksum before proceding
BPI Encryption
RTP HDR
PacketCable RTP Encryption
PacketCable RTP Authentication
cntl/Seq No.
timestamp
SSRC
D
D
D
D
D
D
D
D
MAC
CRC
550
start RTP authenticate
Read timestamp to configure PacketCable key gen for RC4/MMH
552
start RTP encrypt
554
stop PacketCable RTP encrypt/auth
556
verify MAC before proceding
verify chksum before proceding
558

FIG. 8

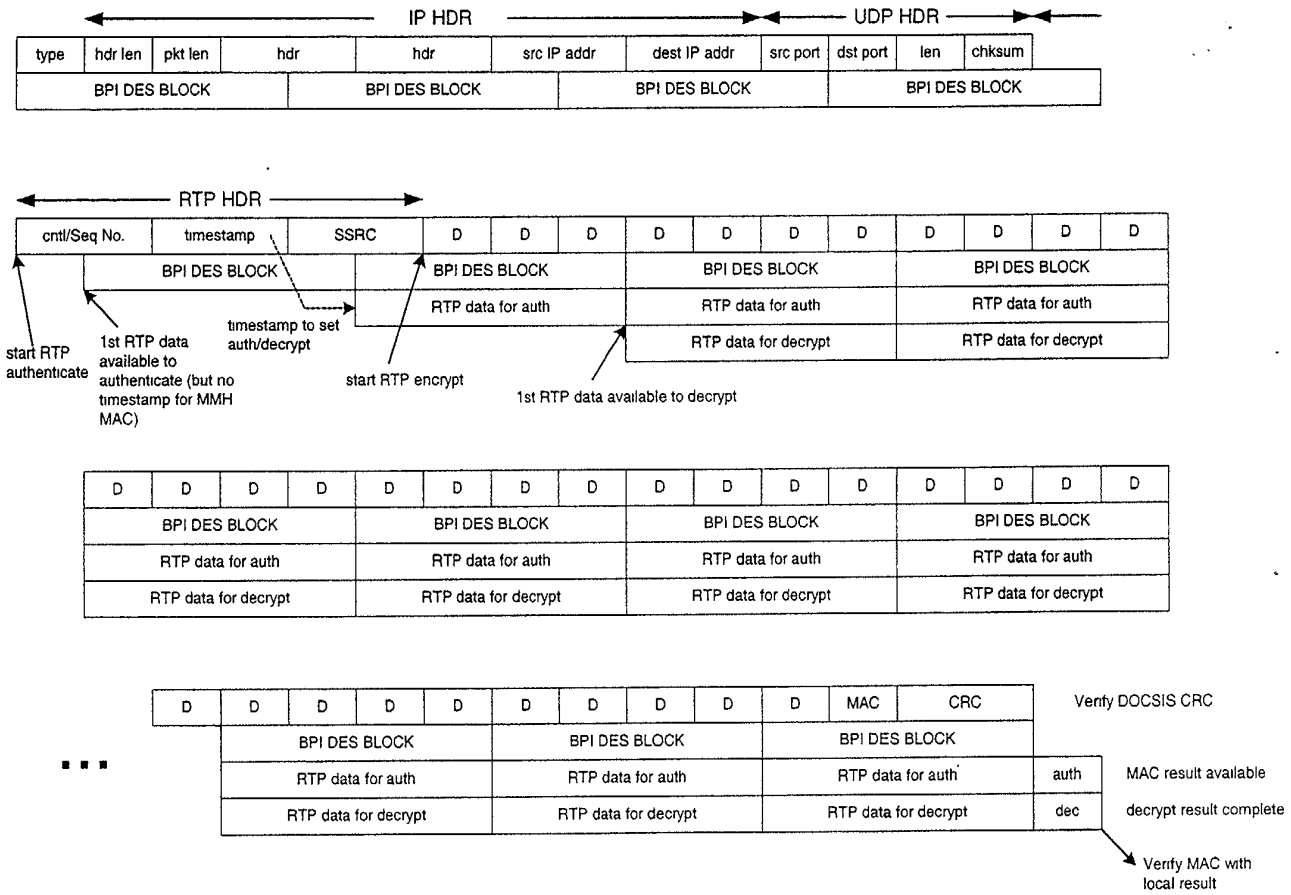
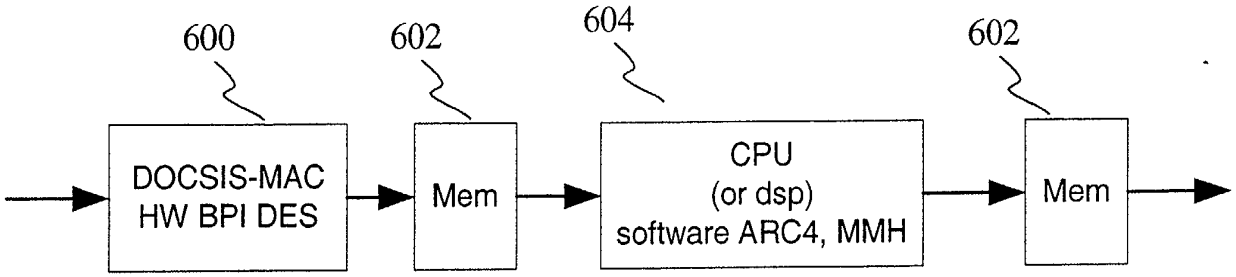
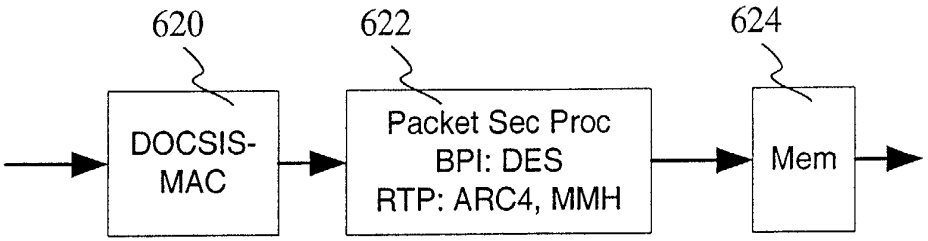

IP HDR
UDP HDR
type
hdr len
pkt len
hdr
hdr
src IP addr
dest IP addr
src port
dst port
len
chksum
BPI DES BLOCK
RTP HDR
cntl/Seq No.
timestamp
SSRC
D
RTP data for auth
RTP data for decrypt
start RTP authenticate
1st RTP data available to authenticate (but no timestamp for MMH MAC)
timestamp to set auth/decrypt
start RTP encrypt
1st RTP data available to decrypt
MAC
CRC
Verify DOCSIS CRC
auth
MAC result available
dec
decrypt result complete
Verify MAC with local result

FIG. 9



Current Process Flow



Converged Security Process Flow

FIG. 10

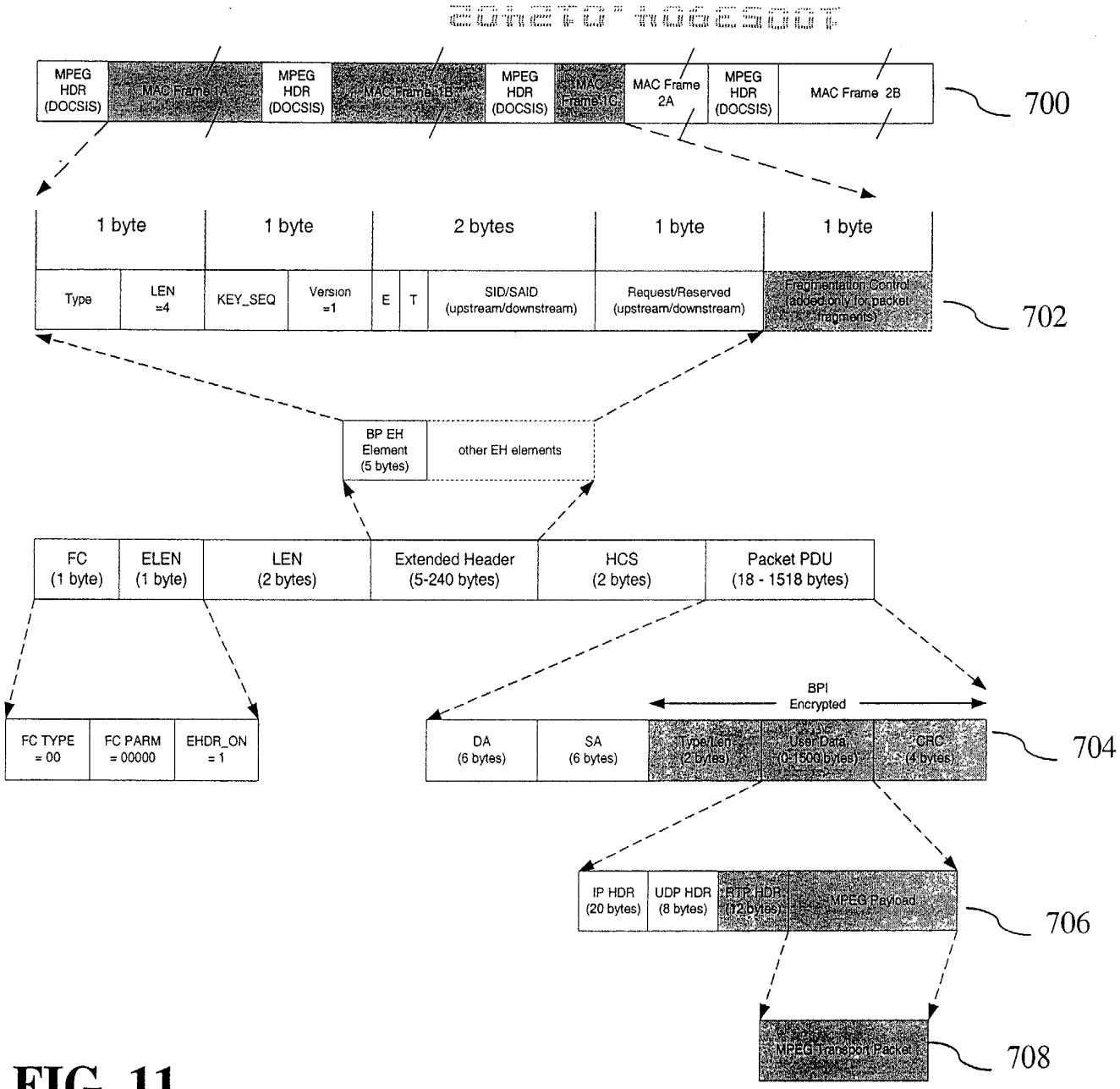

MPEG HDR (DOCSIS)
MAC Frame 1A
MPEG HDR (DOCSIS)
MAC Frame 1B
MPEG HDR (DOCSIS)
MAC Frame 1C
MAC Frame 2A
MPEG HDR (DOCSIS)
MAC Frame 2B
700
1 byte
1 byte
2 bytes
1 byte
1 byte
Type
LEN =4
KEY_SEQ
Version =1
E
T
SID/SAID (upstream/downstream)
Request/Reserved (upstream/downstream)
Fragmentation Control (added only for packet fragments)
702
BP EH Element (5 bytes)
other EH elements
FC (1 byte)
ELEN (1 byte)
LEN (2 bytes)
Extended Header (5-240 bytes)
HCS (2 bytes)
Packet PDU (18 - 1518 bytes)
BPI Encrypted
FC TYPE = 00
FC PARM = 00000
EHDR_ON = 1
DA (6 bytes)
SA (6 bytes)
Type/Len (2 bytes)
User Data (0-1500 bytes)
CRC (4 bytes)
704
IP HDR (20 bytes)
UDP HDR (8 bytes)
RTP HDR (12 bytes)
MPEG Payload
706
MPEG Transport Packet
708

FIG. 11

20170 10e3007

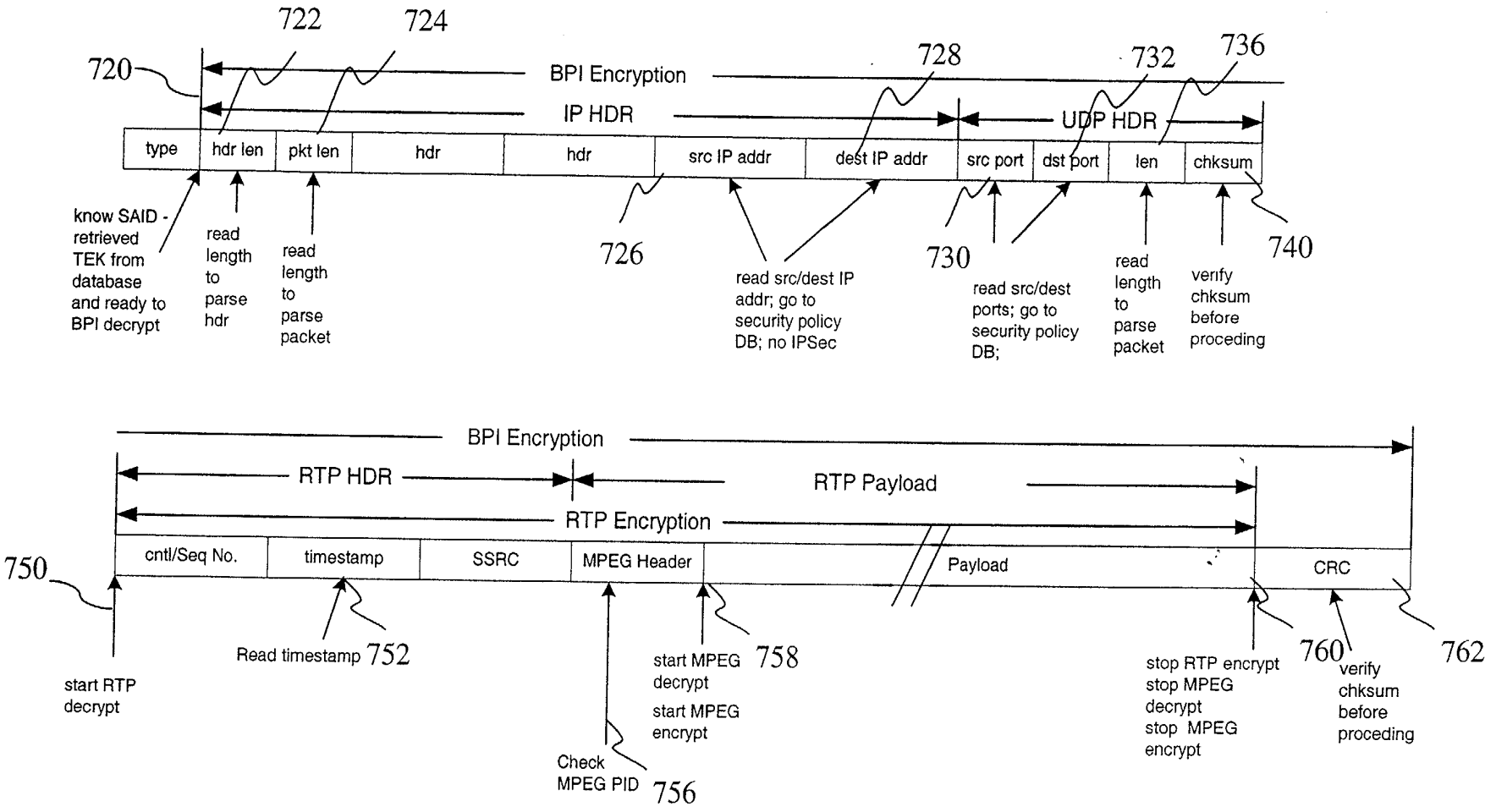


FIG. 12

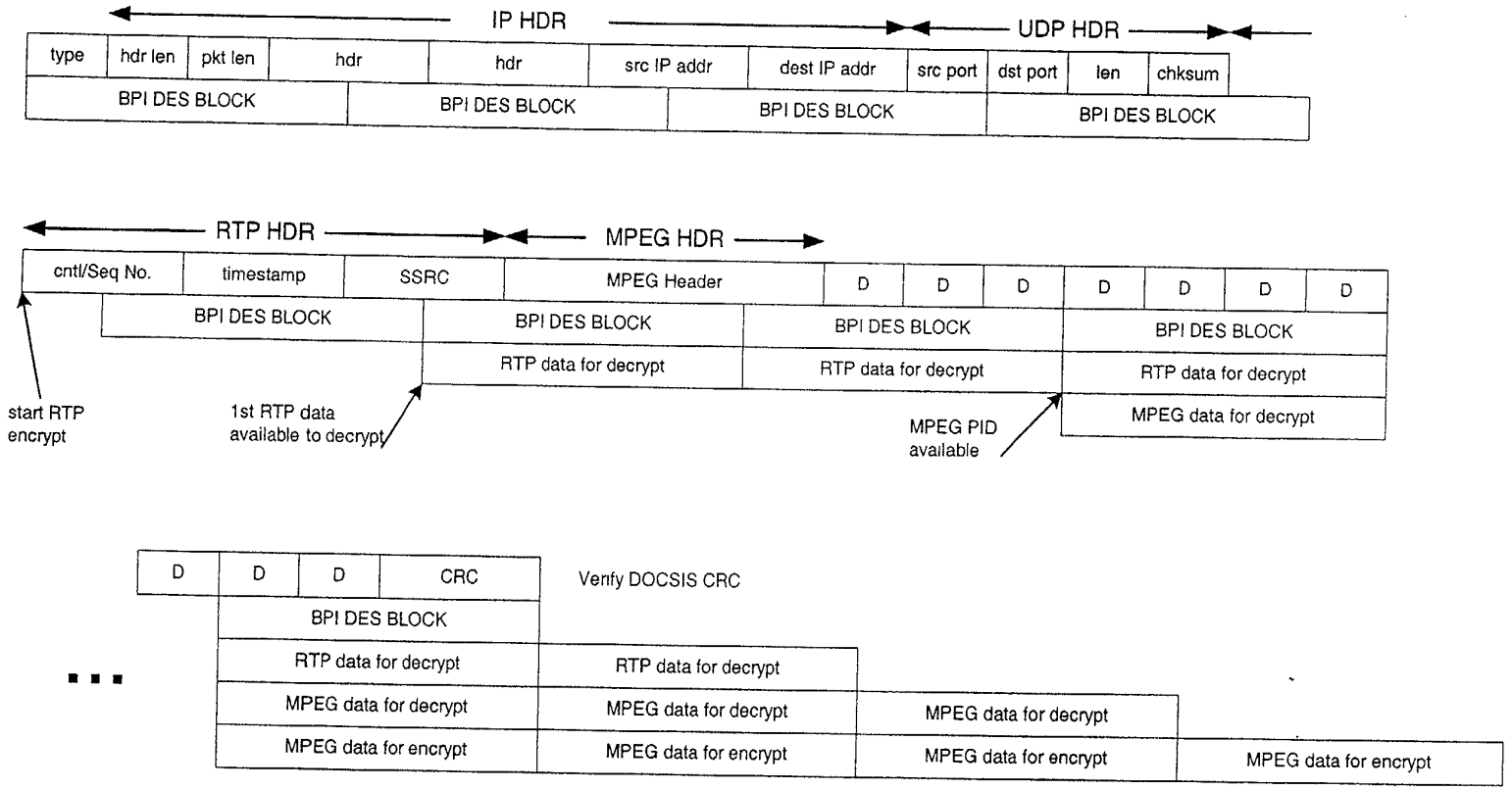

IP HDR
UDP HDR
type
hdr len
pkt len
hdr
hdr
src IP addr
dest IP addr
src port
dst port
len
chksum
BPI DES BLOCK
BPI DES BLOCK
BPI DES BLOCK
BPI DES BLOCK
RTP HDR
MPEG HDR
cntl/Seq No.
timestamp
SSRC
MPEG Header
D
BPI DES BLOCK
RTP data for decrypt
MPEG data for decrypt
start RTP encrypt
1st RTP data available to decrypt
MPEG PID available
CRC
Verify DOCSIS CRC
MPEG data for encrypt

FIG. 13